

On a linear code from a configuration of lines on the affine plane

Ken-ichi SUGIYAMA*

Department of Mathematics and Informatics, Faculty of Science
Chiba University, Japan.

February 1, 2008

Abstract

We will show how to make a linear code from a configuration of affine lines in general position and a suitable set of rational points on it. The number of rational points on our singular curve is beyond the Weil bound and their coordinates are quite easy to compute. We will show a new decoding procedure which originates from the configuration. It is expected our method may correct errors less than almost the minimal distance *itself*, not the half of it.

2000 Mathematics Subject Classification : 11T71, 14G50, 94B27, 94B35, 94B70.

Key words : algebraic-geometric codes, a configuration of lines, decoding.

1 Introduction

In order to make a linear code from a nonsingular projective curve defined over a finite field \mathbb{F}_q (q is a power of a prime p), it should have many rational points. Let X be such a curve of genus g and $P = \{P_1, \dots, P_N\}$ a set of rational points on it. We choose an effective divisor D defined over \mathbb{F}_q whose support is disjoint from P and satisfying

$$2g - 2 < \deg(D) < N.$$

Then the evaluation map

$$\begin{aligned} \mathcal{L}(D) &\xrightarrow{\alpha} \mathbb{F}_q^N \\ \alpha(f) &= (f(P_1), \dots, f(P_N)), \end{aligned}$$

embeds the linear system $\mathcal{L}(D)$ into \mathbb{F}_q^N and let $C(X, D)$ be its image. This is the basic construction of a linear code using the algebraic geometry. It is known

*Cooresponding address : Department of Mathematics and Informatics, Faculty of Science, Chiba University, 1-33 Yayoi-cho Inage-ku, Chiba 263-8522, Japan. e-mail address : sugiyama@math.s.chiba-u.ac.jp

that its dimension is $\deg(D) - g + 1$ and the minimal distance is greater than or equal to $N - \deg(D)$. ([2], §10.6)

But due to Weil, the number of rational points is bounded by

$$1 + q + 2g\sqrt{q},$$

from above. Even though one finds a good curve which attains the Weil bound, it is quite hard to write down its equation explicitly and so is to obtain the coordinates of rational points.

In [1], in order to overcome this difficulty, we have proposed to use a configuration of affine lines on the affine plane and have studied its general properties. In this note we will show a explicit construction of a good linear code from a certain configuration and a suitable set of rational points on it. We will also investigate its property in detail and will discuss a new decoding procedure, which seems to be quite effective.

Let $\{L_1, \dots, L_n\}$ be affine lines in a general position on the affine (x, y) -plane which are defined over \mathbb{F}_q , namely the intersection of every three of them is empty. Let \mathcal{I} be the set of their intersection and we fix a positive integer m . We take mutually distinct \mathbb{F}_q -rational points $\{P_{i1}, \dots, P_{im}\}$ on L_i disjoint from \mathcal{I} . Let d be a positive integer less than both of m and n and we put

$$\mathcal{F}_d = \left\{ \sum_{i+j \leq d} a_{ij} x^i y^j \mid a_{ij} \in \mathbb{F}_q \right\}.$$

Then the evaluation map embeds \mathcal{F}_d into the space of (n, m) -matrices:

$$\mathcal{F}_d \xrightarrow{e} M_{nm}(\mathbb{F}_q), \quad e(f) = (f(P_{ij}))_{ij},$$

and its image is our linear code. The generating matrix can be explicitly computed to be

$$\begin{pmatrix} 1 & x(P_1) & y(P_1) & \cdots & x(P_1)^d & \cdots & y(P_1)^d \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x(P_{nm}) & y(P_{nm}) & \cdots & x(P_{nm})^d & \cdots & y(P_{nm})^d \end{pmatrix}.$$

The dimension of the code is $\frac{(d+2)(d+1)}{2}$ and the minimal distance is greater than or equal to $n(m-d)$ (resp. $m(n-d)$) if $m > n$ (resp. $n > m$). Moreover we have a new decoding procedure which originates from the configuration. It is expected to correct errors less than $n(m-d)$ or $m(n-d)$ if $m > n$ or $n > m$, respectively.

Here is an example to make $\{P_{ij}\}_{ij}$. Let $\{L_1, \dots, L_n, M_1, \dots, M_m\}$ be affine lines in a general position and take P_{ij} as the intersection of L_i and M_j . Then

the minimal distance of the code obtained from $\{L_1, \dots, L_n\}$ and $\{P_{ij}\}_{ij}$ coincides with $n(m-d)$ or $m(n-d)$ if $m > n$ or $n > m$, respectively. Therefore our decoding method may correct errors up to the minimal distance *itself*, not the half of it.

By the Weil bound there are at most $1 + q + (n-1)(n-2)\sqrt{q}$ rational points on a nonsingular projective curve of degree n in the projective plane. But there are $nq - \frac{n(n-1)}{2}$ rational points on our configuration of affine lines. Thus, for fixed n , taking q large enough, the number of rational points on our curve is beyond the Weil bound. Moreover they are quite easy to compute.

2 Notation

We will use the following notation throughout the paper.

- For a finite set X its cardinality will be denoted by $|X|$.

Let V be a vector space over \mathbb{F}_q of a finite dimension. The function from X to V will be denoted by V^X , which is a vector space of dimension $|X|\dim V$.

Example 2.1. $\mathbb{F}_q^{\{1, \dots, N\}}$ is isomorphic to \mathbb{F}_q^N by the linear map:

$$\varphi(f) = (f(1), \dots, f(N)), \quad f \in \mathbb{F}_q^{\{1, \dots, N\}}.$$

Using this we will identify them.

Let Y be a subset of X . Then there is a linear map

$$V^X \xrightarrow{r_Y} V^Y,$$

by restriction. The image of $v \in V^X$ will be denoted by v_Y .

Putting an arbitrary component whose index is not contained in Y to be zero, V^Y may be considered as a subvector space of V^X .

Example 2.2. If one takes a subset Σ of $\{1, \dots, N\}$, \mathbb{F}_q^Σ is identified with a subspace of \mathbb{F}_q^N defined as

$$\{(x_1, \dots, x_N) \mid x_i = 0 \text{ if } i \notin \Sigma\}.$$

By definition the restriction r_Y to V^Y is the identity.

Finally the diagonal Δ_{V^X} of V^X is defined to be the set of functions which take the same value at every element of X :

$$\Delta_{V^X} = \{f \in V^X \mid f(x) = f(x') \text{ for any } x, x' \in X\}.$$

3 A construction of a linear code

Let us fix an n -tuple of affine lines on the affine plane defined by a linear function l_i :

$$l_i = a_i x + b_i y + c_i, \quad a_i, b_i, c_i \in \mathbb{F}_q.$$

and L_i the line defined by l_i . We assume that they are in a general position.

If

$$\begin{pmatrix} a_i & b_i & c_i \\ a_j & b_j & c_j \\ a_k & b_k & c_k \end{pmatrix}$$

is regular, the equation

$$\begin{cases} a_i x + b_i y + c_i = 0 \\ a_j x + b_j y + c_j = 0 \\ a_k x + b_k y + c_k = 0 \end{cases}$$

has no solution and we know the intersection of $\{L_i, L_j, L_k\}$ is empty. This observation shows the following lemma.

Lemma 3.1. *A family of affine lines*

$$\{L_1, \dots, L_N\}$$

is in a general position if every 3×3 -minor of

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ \vdots & \vdots & \vdots \\ a_N & b_N & c_N \end{pmatrix}$$

is regular.

The intersection of L_i and L_j , which is an \mathbb{F}_q rational point, will be denoted by I_{ij} . Let us choose mutually distinct m points $\{P_{i1}, \dots, P_{im}\}$ on L_i which are \mathbb{F}_q rational and not contained in $\{I_{ij}\}_j$. The collection $\{P_{ij}\}_{i,j}$ will be denoted by \mathcal{P} .

Let $\mathbb{F}_q[x, y]$ be the polynomial ring of variables x and y with \mathbb{F}_q -coefficients. For a positive integer d less than m and n , we denote the subspace consisting of polynomials whose degrees are at most d by \mathcal{F}_d . As a base of \mathcal{F}_d we choose

$$\{1, x, y, \dots, x^d, \dots, y^d\}. \quad (1)$$

In particular the dimension of \mathcal{F}_d is

$$\delta = \frac{(d+2)(d+1)}{2}.$$

Now we define *the evaluation map*

$$\mathcal{F}_d \xrightarrow{e} \mathbb{F}_q^{\mathcal{P}} \simeq M_{nm}(\mathbb{F}_q)$$

to be

$$e(f) = (f(P_{ij}))_{ij}.$$

Proposition 3.1. *e is injective.*

In order to prove the proposition we will prepare some notation.

By the lexicographic order, we arrange the indices of \mathcal{P} as

$$((1, 1), \dots, (1, m), \dots, (n, 1), \dots, (n, m)) = (1, \dots, nm), \quad (2)$$

which gives an identification between $M_{nm}(\mathbb{F}_q)$ and \mathbb{F}_q^{nm} . For a subset Σ of \mathcal{P} , composing with the restriction map, the evaluation map induces a linear map:

$$\mathcal{F}_d \xrightarrow{e_\Sigma} \mathbb{F}_q^\Sigma.$$

A subset \mathcal{Q} of \mathcal{P} will be mentioned *effective* if there are distinct $(d+1)$ -members $\{L_{q_1}, \dots, L_{q_{d+1}}\}$ of $\{L_i\}_{1 \leq i \leq n}$ such that the cardinality of $\mathcal{Q} \cap L_{q_\nu}$ is ν . In particular $|\mathcal{Q}|$ is δ .

The **Proposition 3.1** immediately follows from the next proposition.

Proposition 3.2. *For an effective set \mathcal{Q} ,*

$$\mathcal{F}_d \xrightarrow{e_\mathcal{Q}} \mathbb{F}_q^\mathcal{Q}.$$

is an isomorphism.

Proof. Since the source and the target have the same dimension it is sufficient to show $e_\mathcal{Q}$ is injective. Suppose $f \in \mathcal{F}_d$ satisfies $e_\mathcal{Q}(f) = 0$ and let f_ν be the restriction of f to L_{q_ν} . Taking a linear parametrization of L_{q_ν} , f_ν is a polynomial of one variable whose degree is at most d . Let $\{Q_{\nu,1}, \dots, Q_{\nu,\nu}\}$ be the intersection of \mathcal{Q} and L_{q_ν} . We will show the following claim by an induction for ν .

Claim. The product $l_{q_{d+1}} \cdots l_{q_{d+1-\nu}}$ divides f for $0 \leq \nu \leq d$.

For $\nu = 0$ the assumption implies that f_{d+1} vanishes at mutually distinct $(d+1)$ -points $\{Q_{d+1,1}, \dots, Q_{d+1,d+1}\}$. Therefore f_{d+1} vanishes because its degree is at most d . This implies that $l_{q_{d+1}}$ divides f .

Let us assume the claim is true for $\nu = i$. We know f_{d-i} vanishes at $\{Q_{d-i,1}, \dots, Q_{d-i,d-i}\}$ by the assumption. Moreover since $l_{q_{d+1}} \cdots l_{q_{d+1-i}}$ divides f , f_{d-i} also vanishes on the intersection of $L_{q_{d+1}} \cup \dots \cup L_{q_{d+1-i}}$ and $L_{q_{d-i}}$,

which is $\{I_{q_{d-i}, d-i+1}, \dots, I_{q_{d-i}, d+1}\}$. Therefore f_{d-i} vanishes at mutually distinct $(d+1)$ -points and is zero by the reason of degree. This implies that f is divided by $l_{q_{d-i}}$.

The claim shows that $l_{q_{d+1}} \cdots l_{q_1}$ divides f , but since the degree f is at most d , it should be zero.

□

We will consider the image of the evaluation map $e(\mathcal{F}_d)$ as a linear code.

Using the base (1) and the lexicographic order (2) the evaluation map has the following matrix representation:

$$E = \begin{pmatrix} 1 & x(P_1) & y(P_1) & \cdots & x(P_1)^d & \cdots & y(P_1)^d \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x(P_{nm}) & y(P_{nm}) & \cdots & x(P_{nm})^d & \cdots & y(P_{nm})^d \end{pmatrix}.$$

It is nothing but the generating matrix of the code.

4 How to decode a message

Let $\mathcal{E}_{n,m,d}$ be the family of effective sets. Its cardinality is computed to be

$$|\mathcal{E}_{n,m,d}| = \prod_{i=0}^d (n-i) \cdot \binom{m}{d+1-i}.$$

For an effective set $\mathcal{Q} \in \mathcal{E}_{n,m,d}$, extracting the corresponding row vectors from E , we obtain its $\delta \times \delta$ -minor $E_{\mathcal{Q}}$. Then **Proposition 3.2** shows it is a regular matrix. Using column vectors:

$$\mathbf{x} = \begin{pmatrix} 1 \\ x \\ y \\ \vdots \\ x^d \\ \vdots \\ y^d \end{pmatrix}, \quad \mathbf{a} = \begin{pmatrix} a_{00} \\ a_{10} \\ a_{01} \\ \vdots \\ a_{d0} \\ \vdots \\ a_{0d} \end{pmatrix},$$

$$f = \sum_{i+j \leq d} a_{ij} x^i y^j \in \mathcal{F}_d$$

has an expression

$$f = \mathbf{x}^t \cdot \mathbf{a}.$$

Moreover the image of evaluation map of f is given by

$$e(f) = E \cdot \mathbf{a}.$$

Now extracting components from both side whose indices are contained in \mathcal{Q} , we obtain

$$e(f)_{\mathcal{Q}} = E_{\mathcal{Q}} \cdot \mathbf{a},$$

and

$$\mathbf{a} = E_{\mathcal{Q}}^{-1} \cdot e(f)_{\mathcal{Q}}.$$

Thus we have proved

Proposition 4.1. *For an element $\mathbf{c} \in e(\mathcal{F}_d)$, the vector $(E_{\mathcal{Q}}^{-1} \cdot \mathbf{c}_{\mathcal{Q}})_{\mathcal{Q}}$ is contained in the diagonal $\Delta_{(\mathbb{F}_q^\delta)^{\mathcal{E}_{n,m,d}}}$ of $(\mathbb{F}_q^\delta)^{\mathcal{E}_{n,m,d}}$. Moreover choosing arbitrary $\mathcal{Q} \in \mathcal{E}_{n,m,d}$, we have*

$$\mathbf{c} = E \cdot E_{\mathcal{Q}}^{-1} \cdot \mathbf{c}_{\mathcal{Q}}.$$

Let $\mathbf{c} = E \cdot \mathbf{a}$ be an element of the code. We choose an arbitrary error vector $\mathbf{e} \in \mathbb{F}_q^{nm}$ and set

$$\mathbf{c}' = \mathbf{c} + \mathbf{e},$$

which may be considered as a received message. We want to estimate the probability to hold

$$E_{\mathcal{Q}}^{-1} \mathbf{c}'_{\mathcal{Q}} = E_{\mathcal{Q}'}^{-1} \mathbf{c}'_{\mathcal{Q}'} \quad (3)$$

for $\mathcal{Q}, \mathcal{Q}' \in \mathcal{E}_{n,m,d}$. If we put $\delta_{\mathcal{Q}} = E_{\mathcal{Q}}^{-1} \mathbf{e}_{\mathcal{Q}}$ and $\delta_{\mathcal{Q}'} = E_{\mathcal{Q}'}^{-1} \mathbf{e}_{\mathcal{Q}'}$ respectively, **Prpposition 4.1** shows that (3) is equivalent to

$$\delta_{\mathcal{Q}} = \delta_{\mathcal{Q}'}.$$

The probability to hold this identity is

$$q^{-|\mathcal{Q} \ominus \mathcal{Q}'|},$$

where $\mathcal{Q} \ominus \mathcal{Q}' = \mathcal{Q} \cup \mathcal{Q}' \setminus (\mathcal{Q} \cap \mathcal{Q}')$. This is very small if \mathcal{Q} and \mathcal{Q}' are different and if q is sufficiently large. Therefore it is expected that the following decoding procedure should be effective.

How to decode

Take q large and let $\mathbf{m} \in \mathbb{F}_q^{nm}$ be a received vector.

1. Compute $\mathbf{a}_{\mathcal{Q}} = E_{\mathcal{Q}}^{-1} \mathbf{m}_{\mathcal{Q}}$ for each effective set \mathcal{Q} .
2. If at least two of them coincide, search an element of $\{\mathbf{a}_{\mathcal{Q}}\}_{\mathcal{Q} \in \mathcal{E}_{n,m,d}}$ of the largest multiplicity. On the contrary if they are different each other, we think it is impossible to decode \mathbf{m} .
3. Let \mathbf{a} be the vector caluculated in **Step 2**. Then the correct message should be $E \cdot \mathbf{a}$.

For distinct effective sets \mathcal{Q} and \mathcal{Q}' , the previous estimate implies that if $\mathbf{m}_{\mathcal{Q}}$ or $\mathbf{m}_{\mathcal{Q}'}$ contains an error it should be quite rare that $\mathbf{a}_{\mathcal{Q}}$ coincides with $\mathbf{a}_{\mathcal{Q}'}$. But if \mathbf{m} contains too many errors, it may happen that it is impossible to decode the message vector because every two of $\{\mathbf{a}_{\mathcal{Q}}\}_{\mathcal{Q} \in \mathcal{E}_{n,m,d}}$ may not coincide. In the next section we will estimate the number of errors to be corrected.

5 An estimate of the number of errors which may be corrected

Let R_{nm} be the following $n \times m$ rectangle with grids:

$(1, 1)$		\dots		$(1, m)$
\vdots		\ddots		\vdots
$(n, 1)$		\dots		(n, m)

Corresponding the grid (i, j) to P_{ij} , one may identify it with $\mathcal{P} = \{P_{ij}\}_{i,j}$. A subset T of R_{nm} will be mentioned as *a tableau* if it satisfies the following condition:

If (i, j) is contained in T , so is (k, l) for $1 \leq k \leq i$ and $1 \leq l \leq j$.

Here is a picture which illustrates the condition. \heartsuit is a grid contained in a tableau.

		\heartsuit				

 \Rightarrow

\heartsuit	\heartsuit	\heartsuit			
\heartsuit	\heartsuit	\heartsuit			
\heartsuit	\heartsuit	\heartsuit			

In general for a subset Σ of R_{nm} , we denote the number of grids contained in it by $\sigma(\Sigma)$.

Example 5.1. 1. (Regular tableau) The regular tableau of size l is

$(1, 1)$		\dots		$(1, l)$
\vdots				
$(l, 1)$				

which will be denoted by R_l . We have

$$\sigma(R_l) = \frac{l(l+1)}{2}.$$

2. $(T_{k,l})$ The following tableau will be denoted by $T_{k,l}$:

$(1,1)$	\cdots	$(1,l)$	\cdots	$(1,m)$
\vdots	\ddots	\vdots	\ddots	\vdots
$(k,1)$	\cdots	(k,l)	\cdots	(k,m)
\vdots	\ddots	\vdots		
$(n,1)$	\cdots	(n,l)		

We have

$$\sigma(T_{k,l}) = ln + km - kl.$$

Let \mathcal{C} be a subset of R_{nm} . We will consider a sufficient condition so that it contains at least two effective sets. Changing the numbering of lines and points, we may assume \mathcal{C} is a tableau.

Lemma 5.1. *Let \mathcal{C} be a tableau. If it contains R_{d+1} and satisfies*

$$\sigma(\mathcal{C}) > \sigma(R_{d+1}) = \frac{(d+2)(d+1)}{2},$$

it contains at least two effective sets.

Since one can prove it by inspection, we only show the simplest example of $d = 2$:

If \mathcal{C} is

,

it contains the following two effective sets which are marked by \heartsuit :

\heartsuit	\heartsuit	\heartsuit
\heartsuit	\heartsuit	
\heartsuit		

and

\heartsuit	\heartsuit	\heartsuit
\heartsuit	\heartsuit	
\heartsuit		

Lemma 5.2. *If a tableau T does not contain R_{d+1} , we have*

$$\sigma(T) \leq \text{Max}\{f(k) \mid 1 \leq k \leq d+1\},$$

where

$$f(x) = x^2 + (m - n - d - 2)x + (n + 1)(d + 1) - m.$$

Proof. The assumption implies that there is k with $1 \leq k \leq d+1$ such that the grid $(k, d+2-k)$ is not contained in T . Then by the definition of a tableau, we see T is contained in $T_{k-1, d+1-k}$. Here is a picture which illustrates our situation:

♥	♥	♥	♥	♥	♥	
♥	♥	♥	♥			
♥	♥	♥	♠			
♥	♥	♥				
♥	♥					
♥	♥					

Here ♥ are grids contained in T and ♠ is one at $(k, d+2-k)$. Hence we have

$$\begin{aligned} \sigma(T) &\leq \sigma(T_{k-1, d+1-k}) \\ &= f(k) \\ &\leq \text{Max}\{f(k) \mid 1 \leq k \leq d+1\}. \end{aligned}$$

□

Corollary 5.1. *Suppose that a tableau T satisfies*

$$\sigma(T) > \text{Max}\{f(k) \mid 1 \leq k \leq d+1\},$$

then it contains R_{d+1} .

Notice that

$$f(1) = nd, \quad f(d+1) = md.$$

If m or n is greater than or equal to $d+2$ respectively, since d is a positive integer, we have

$$\begin{aligned} f(d+1) &= md \\ &\geq d(d+2) \\ &\geq \frac{(d+2)(d+1)}{2} = \sigma(R_{d+1}), \end{aligned}$$

or

$$f(1) = nd \geq \sigma(R_{d+1}),$$

respectively. This shows

$$\text{Max}\{f(k) \mid 1 \leq k \leq d+1\} \geq \sigma(R_{d+1}).$$

Combining **Lemma 5.1** and **Corollary 5.1** we obtain the following theorem.

Theorem 5.1. *Suppose that m or n is greater than or equal to $d+2$. If a subset \mathcal{C} of R_{nm} satisfies*

$$\sigma(\mathcal{C}) > \text{Max}\{f(k) \mid 1 \leq k \leq d+1\},$$

it contains at least two effective sets.

From now we choose m and n so that one of them is greater than or equal to $d+2$.

For a vector $\gamma = (\gamma_1, \dots, \gamma_{nm}) \in \mathbb{F}_q^{nm}$ its *support* is defined to be

$$\text{supp}(\gamma) = \{i \mid \gamma_i \neq 0\},$$

and let $\nu(\gamma)$ be its cardinality. Let \mathbf{m} be a received vector. It can be written as

$$\mathbf{m} = \mathbf{c} + \mathbf{e},$$

where \mathbf{c} is an element of the code and \mathbf{e} is an error. Let \mathcal{C} be the complement of the support of \mathbf{e} . **Theorem 5.1** and **Proposition 4.1** show, in the decoding procedure in the previous section, if $\nu(\mathbf{e})$ is less than $nm - \text{Max}\{f(k) \mid 1 \leq k \leq d+1\}$, at least two of $\{E_{\mathcal{Q}}^{-1} \cdot \mathbf{c}_{\mathcal{Q}}\}_{\mathcal{Q} \in \mathcal{E}_{n,m,d}}$ coincide. Therefore it is expected that our decoding procedure can correct errors less than $nm - \text{Max}\{f(k) \mid 1 \leq k \leq d+1\}$.

Now we will estimate the minimal distance. Let \mathbf{c} be an element of the code and T the complement of its support. As before we may assume that T is a tableau. **Proposition 4.1** and **Corollary 5.1** show if $\sigma(T) = nm - \nu(\mathbf{c})$ is greater than

$$\text{Max}\{f(k) \mid 1 \leq k \leq d+1\},$$

\mathbf{c} should be zero. Thus we know

$$\nu(\mathbf{c}) \geq nm - \text{Max}\{f(k) \mid 1 \leq k \leq d+1\}$$

for every nonzero code vector \mathbf{c} , which implies the minimal distance of $e(\mathcal{F}_d)$ is greater than or equal to $nm - \text{Max}\{f(k) \mid 1 \leq k \leq d+1\}$.

Notice that, choosing \mathcal{P} suitably, it is possible to construct a code whose minimal distance is just $nm - \text{Max}\{f(k) \mid 1 \leq k \leq d+1\}$.

In fact let $\{L_1, \dots, L_n, M_1, \dots, M_m\}$ be a family of affine lines in a general position which are defined by linear functions whose coefficients are in \mathbb{F}_q , $\{l_1, \dots, l_n, m_1, \dots, m_m\}$, respectively. Let P_{ij} be the intersection of L_i and

M_j . Suppose $\text{Max}\{f(k) \mid 1 \leq k \leq d+1\}$ is obtained at $k = k_0$. If we take a polynomial p of degree d to be

$$p = \prod_{i=1}^{k_0-1} l_i \cdot \prod_{j=1}^{d+1-k_0} m_j,$$

it is easy to see the complement of the support of $e(p)$ is $T_{k_0-1, d+1-k_0}$. Thus we have

$$\begin{aligned} \nu(e(p)) &= nm - \sigma(T_{k_0-1, d+1-k_0}) \\ &= nm - \text{Max}\{f(k) \mid 1 \leq k \leq d+1\}. \end{aligned}$$

Here are some examples.

- Example 5.2.** 1. Suppose m is greater than n . Then it is easy to see that $f(1) = nd$ is the maximum. Therefore it is expected that our decoding procedure may correct errors less than $n(m-d)$.
2. On the contrary suppose n is greater than m . Then $f(d+1) = md$ is the maximum and it is expected that our decoding procedure may correct errors less than $m(n-d)$.

Acknowledgements The author is partially supported by the Grand-in-Aid for Scientific Research (C) No.18540203, the Ministry of Education, Culture, Sports, Science and Technology, Japan.

References

- [1] K. Shibaki and K. Sugiyama. A linear code from a configuration of affine lines on the projective plane. Submitted (2005).
- [2] van Lint. Introduction to Coding Theory, volume 86 of *GTM*. Springer-Verlag, Berlin-Heidelberg, New York (1998).